PCT/AU2004/000762

Australian Government

Patent Office
Canberra

I, JULIE BILLINGSLEY, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2003902911 for a patent by THE COMMONWEALTH OF AUSTRALIA as filed on 11 June 2003.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Eighteenth day of June 2004

J. Billingsley

JULIE BILLINGSLEY
TEAM LEADER EXAMINATION
SUPPORT AND SALES

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

54567 HKS:LR

P/00/009
Regulation 3.2

AUSTRALIA
Patents Act 1990

ORIGINAL

PROVISIONAL SPECIFICATION FOR AN INVENTION ENTITLED

Invention Title: Credential Communication Device

Name of Applicant: The Commonwealth of Australia

Address for Service: **COLLISON & CO.** 117 King William Street, Adelaide, S.A. 5000

The invention is described in the following statement :

TECHNICAL FIELD

This invention relates to the field of personal identification and credential communication.

BACKGROUND ART

There are many examples of authentication devices and electronic methods of credential exchange. These typically involve a trade-off between security, flexibility and ease of use. For example, a smart card transaction requiring that the card be inserted into a reader gives high confidence that the communication between the card and the reader involves only those two parties, but is relatively inconvenient. A transaction involving a wireless reader such as that used in some subway ticketing system does not even require the user to take the card from their wallet, but unauthorised and undetected third party involvement would be quite straightforward.

Further, these devices typically require an access point where a network function or access point function undertakes the credential processing. Thus a client appliance identifies itself to a master device which then applies pre-selected protocols to the transaction based on that identification. Peer to peer authentication is not catered for. For example, in the case of a credit card or smart card, they are placed within an ATM or other network active receptacle which undertakes the required processing. No transaction is possible between such cards in the absence of a network.

Nor is mutual suspicion credential exchange possible. The client must trust the master and identify itself to the master. This is not a problem where the master device is part of a fixed installation which serves to establish that it is bona fide. This becomes much more problematic when both devices are mobile.

In addition, the user selectable features are a part of the network rather than a property of the card itself.

There is a need for a limited use "business card" and identification token for organisations where personnel may not necessarily know each other but need to know role information such as security clearances, financial approval authorisations, access rights or medical treatment records. It is useful to provide for token to token

exchange which establishes user and organisation selectable bona fides of the two parties.

In this process, the touching of the tokens or rather the very close proximity of the tokens must be such that each user can be assured that only those wands are participating in the process. Otherwise spoofing may be possible by third party wireless systems acting in variations of classic "man in the middle" or classic "hijack" attacks.

For example, in the Defence domain, two people who meet without formal notification of clearance details but with such tokens could exchange credentials which were signed by the Defence Certification Authority and could therefore calculate the level of information they were permitted to discuss.
In a hospital a doctor could authorise a drug treatment by signing an order, and could check that the doctor had prescribe rights at that hospital.

DISCLOSURE OF THE INVENTION

In one form of the invention, although this need not be the only of the broadest form, it can be said to reside in a set of devices where a first of the devices is adapted to hold information in an electronic storage and effect transmission of such information upon a triggering of such transmission, and a second device is adapted to hold data in an electronic storage and adapted to receive transmissions from said first device and effect a comparison of such received data with that being held by said second device and when such received data is matching preselected criteria effect an output signal to this effect, the respective devices being adapted to effect a transmission and receiving between the devices only when in a selected range of distance apart or when touching.

In preference said devices are adapted to effect credential accreditation information. In preference, the devices have a range of transmission and reception such that they will only transmit and receive at least some data only when in such physical proximity as to effectively exclude the possibility of third party involvement in the transaction.

In a further form of the invention, it can be said to reside in a credential exchange device, said device including a proximity conductor adapted to transfer at least some data only when in such physical proximity to a second credential exchange

device as to effectively exclude the possibility of third party involvement in the transaction.

In a further form of the invention, it may be said to reside in a credential communication device including at least one proximity conductor adapted to transfer at least some data only when in such physical proximity to a second credential exchange device as to effectively exclude the possibility of third party involvement in the transaction, said data being adapted to effect trusted mutual recognition between the device and the second device, without reference to a third party.

In preference, the credential communication device is adapted to require a participant to authenticate their identity immediately before communication with the second device.

In preference the credential communication device is adapted to accept identity authentication by the keying of a pass code into the device.

In preference, the credential communication device is adapted to accept identity authentication by use of a biometric authentication apparatus.

In preference the proximity connector is an induction connection.

In preference, the induction connection is effected by a RF transceiver of such power as to require the physical proximity to be such as approximates physical touch.

In preference the power setting for the proximity conductor is settable so that sufficient power is available to transmit and receive preamble data before physical contact is established, and at the time when physical contact or close proximity is required the power setting is reduced to a level which enures that such close proximity is assured.

In preference, the proximity conductor includes means to detect that physical touch is being maintained between the device and the second device, the device further adapted to transfer some data only when such touch is detected.

In preference the means to detect physical touch is a pressure sensor.

In preference the induction connector is protected from physical or environmental damage by thin layer or shell of material.

In preference, the device includes means to communicate the results of credential verification.

In preference said communication means includes at least one trusted light indicator.

In preference said communication means includes at least three separately identifiable light indicators.

In preference said light indicators are formed as bands around the device to facilitate visibility from multiple angles.

In preference said light indicators are light emitting diodes.

In preference, the device further includes a trusted alpha-numeric display.

In preference the device further includes a biometric authentication apparatus.

In preference said biometric authentication apparatus is a fingerprint scanner.

In preference the device further includes means for receiving wireless transmissions from a distance further than the range of the proximity conductor.

In preference the proximity conductor is a bulbous structure, permitting momentary contact with a second device from a variety of angles.

In preference the device is approximately cylindrical.

In preference, in the alternative, the proximity conductor is located on the shaft of a cylinder, permitting momentary contact with a second device from a variety of angles.

In a further form of the invention, it can be said to reside in a method for mutual suspicion credential exchange including the steps of:
positioning a credential exchange device to touch or come into close proximity with

a second such device,
the credential exchange device transmitting data to and receiving data from the second device,
the credential exchange device processing received data to determine the credential status of the second device,
the credential exchange device outputting the results of the credential determination.

In a further form of the invention, it can be said to reside in a method for mutual suspicion credential exchange including the steps of:
providing each participant with a credential exchange device
loading the credential exchange device with credential data relevant to a user,
each participant operating their device to seek appropriate credential data from a second device,
each participant positioning their device to touch or come into close proximity with a second device,
each device transmitting data to and receiving data from a second device,
each device processing received data to determine the credential status of the second device,
each device outputting the results of the credential determination.

In preference the method further includes the steps of communicating an organisational mandatory security policy to the credential exchange device, and the device applying said mandatory security policy to the data transmitted to the second device. This communication may be restricted to being a one-off process performed when the device is manufactured or first activated.

In preference the method further includes the steps of communicating a user discretionary security policy to the credential exchange device, and the device applying said user discretionary security policy to the data transmitted to the second device. This communication may be restricted to being a one-off process performed when the device is manufactured or first activated.

In preference a mandatory security policy may be communicated to the credential communication device by means localised to the particular location in which the device is operating.

In preference, said policy communication is by secure wireless means.

Trusted appliances which are able to communicate securely together in a manner such that no other device can intrude are known as an ensemble. There can be only one appliance of each type in an ensemble.

In preference the credential communication device is a component in a mutually authenticated ensemble of devices where it may signal a trusted remote visual display device to display data.

In preference the remote visual display device is a badge display.

In preference, the method of credential exchange includes the step of the credential communication device signalling via secure wireless means to the remote visual display means in its own ensemble a visual depiction of the participant associated with the second device.

In a further form of the invention, it may be said to reside in a method for rapid verification of the credentials for a group of participants by a guard including the steps of:

providing each participant and the guard with a credential communication device, said device including a proximity conductor adapted to transfer at least some data only when in such physical proximity to a second credential exchange device as to effectively exclude the possibility of third party involvement in the transaction said device further including memory means and processing means and output means,

loading each participant's credential communication devices with data including the identity and credentials of the participant,

operating the guard's device to cause it to seek appropriate identity or credential data from a participant's device,

positioning each participant's device to touch or come into close proximity with the guard's device,

transmitting data and receiving data between the guard's and the participant's devices,

the guard's device processing received data to determine the credential status of the participant's device,

the guard's device outputting the results of the credential determination.

In preference, a passive device is provided to extend the area in which proximity to the guard's device is sufficient for the proximity conductor to operate.

In preference the passive device is a waveguide, adapted to allow the guard's credential communication to be inserted into it.

In preference, each participant passes their credential communication device through the waveguide to communicate their credentials.

In preference the guard's device is a component in an ensemble including a remote visual display device.

In preference, the method of credential verification includes the step of the guard's credential communication device signalling via secure wireless means to the remote visual display means in its own ensemble a visual depiction of the participant associated with the participant's device.

Trusted appliances which are able to communicate securely together in a manner such that no other device can intrude are known as an ensemble. There can be only one appliance of each type in an ensemble.

In a further form of the invention the credential communication device is a component in a mutually authenticated ensemble of devices where it may signal a trusted remote visual display device to display data.

In preference the remote visual display device is a badge display.

In a preferred embodiment the credential exchange device has a cylindrical form factor and is referred to as a wand. The wand is a portable tamper resistant trusted device which is used for personal identification, credential warrants, and credential exchange. In a preferred embodiment of the wand it would comprise a handheld device with an inductive connector, one or more trusted input switches, one or more trusted light displays such as a light "bands" to permit viewing from multiple angles, a trusted display such as a transflective backlightable LCD display, an untrusted wheel press button, an untrusted audio generator, and a wireless network interface such as Bluetooth or 802.11 ethernet. In addition, wands may be fitted with an optional light meter which can be used to detect when backlighting is needed in an automatic fashion.

In a preferred embodiment of the wand it may choose to use its wireless interface to signal via trusted means another audio device such as a wireless speaker device "button" to generate audio tones and signals.

For practical use the wand should be manufactured to be easily held by the hand and to be stored in a garment pocket. In a preferred embodiment of the wand it may be constructed in the form of a cylinder with the inductive connector at one end covering the tip (typically bulbous shaped), and optionally parts of the cylinder side. This permits ease of momentary connection between wands from a variety of angles.

The light bands running around a circumference of the cylinder can be manufactured via a variety of methods. One typical method is to implement a number of LED device around such a circumference.

A user must authenticate to the wand before use. In a preferred embodiment of the device either a PIN style number can be entered via the trusted input keys, or through an embedded biometric element such as a fingerprint reader, or a combination. After authentication the user has a certain amount of time to undertake the transaction before the device "times out" and re-authentication is required. For wands which have an embedded wireless element, a secure (e.g encrypted with authentication functions) "heartbeat" signal can be received from other trusted devices to delay activation of the timeout.

The most typical use of the wand in a defence context is to check each other's clearances and identity without the intervention of a third party.

For example, two people may meet for various discussions. During the course of these discussions, it becomes apparent that both parties may benefit from a discussion at the secret level on a particular project. Each party may then undertake the following process:

a) Authenticate to their respective wands;

b) Via manipulation of the trusted buttons or wheel each selects a question to ask the other wand which in this case is do they have secret clearances;

c) Each party touches wands for a period of time until the wand signals via a visual means such as the light bands or an audio tone that sufficient data has been transferred between the wands;

d) The wands then processes the data and signals to the respective user either success or failure of whether the other party has a secret clearance. This signalling can be either the trusted band lights, or on the trusted visual display, or a combination. Note that an audio tone is insufficient as this could be spoofed by a number of means.

The touching of the tokens or rather the very close proximity of the tokens must be such that each user can be assured that only those wands are participating in the process.

In order to optimise the data transfer point to point the power settings for the proximity conductor can be settable so that preamble data can be transmitted and received and at the time requirement for close physical proximity the power settings reduced.

The process above can be augmented in a number of ways. For example, as part of the mutual authentication process the wand could transmit via a wireless interface the visual identity of the other party to a "badge" device. The badge device, is a trusted device which has an electronic display and wireless means. Via a secure protocol, it can authenticate and transmit and receive data from a specific wand. Trusted appliances which are able to communicate securely together in a manner such that no other device can intrude are known as an ensemble. There can be only one appliance of each type in an ensemble. In the case of visual checking, the wand transmits information to the active badge appliance in its ensemble. The visual contains a visual identity of the other party. Note that it is essential that the visual transmitted to its ensemble partner is that of the other party, otherwise it may be possible to introduce a spoofing attack.

A further possible augmentation is to add a pressure sensitive surface or membrane to the inductive connector so that actual physical contact with each wand is detected as part of the process. Although the threat is small, this prevents high energy RF devices from simulating very close proximity to another device.

While the input switched can be used in a combination method to provide some form of PIN style authentication, in a preferred embodiment of the wand, it would be fitted with a biometric device such as a fingerprint reader to form part of the user authentication requirement to the wand.

Each wand can contain a user discretionary security policy, and an organisational mandatory security policy.

The mandatory security policy restricts what the user can transact with other wands. For example, a user may wish to disclose they have a Top Secret clearance to another wand holder. However, the mandatory security policy loaded in the wand may state that disclosure of Top Secret clearances can only be disclosed to wand holders who are Australian citizens. If the user selects Top Secret for disclosing, and a transaction with a wand held by a foreign holder takes place, the mandatory security policy may override the user's selection and disclose only a secret level clearance.

A user discretionary security policy can be used for the user to set defaults. For example, if a wand touch takes place without specific user selections, then a standard Secret level clearance may be disclosed to the other party, despite the wand user holding a Top Secret clearance.

The mandatory security policy can also operate when attendees on entering a room their wands are notified by a trusted wireless device in the room that the room can only hold conversation at, say, the secret level. This mandatory security policy may then override wand settings or transactions. Alternatively, a user may request the current security context by manipulating the wand to search for and obtain any mandatory requirements from other trusted devices. For example, a trusted device located in a meeting room may be broadcasting the security context that the room is equipped to handle conversations up to the secret level via a wireless interface and that no one is to exchange credentials above this level. The broadcast is via encrypted, authenticated protocols which can be verified by wands. On entering the room, an attendee's wand receives this broadcast and matches to the policy. If an attendee attempts to exchange, say, notification of Top Secret clearances with other attendee's wand, the wand will refuse to do so.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described with the assistance of drawings in which:

Figure 1 is a representation of the credential communication device in a wand form factor.

Figure 2 shows two wands in use.

Figure 3 shows the remote visual display apparatus in a badge form factor.
Figure 4 shows an embodiment including a waveguide for extending the area in which close proximity contact is possible.
Figure 5 shows the embodiment of Fig 4 in use.

BEST METHOD FOR CARRYING OUT THE INVENTION

Fig 1 shows a credential communication device constructed according to the invention. It has a cylindrical, tamper resistant casing 1 and is of a size to be conveniently held in the hand or stored in a garment pocket. This size and shape is referred to as the wand form factor, and such a device as a wand.

The wand includes a proximity conductor in the form of an inductive connector 2, which is situated at the bulbous end of the wand in order to facilitate ease of touching to other devices.

The wand also includes a transreflective backlightable LCD display 3 and an untrusted audio generator for output. Further output options are provided by three light bands 6 which encirle the body of the wand. These are each made up of multiple light emitting diodes.

For data input, the device has a combined jog wheel and press button 4 and three press buttons 5.

Wireless communication with the wand is provided by an 802.11 ethernet connection. In a further embodiment, this wireless communication link is provided by a Blue tooth interface. It will be appreciated that any proprietary or non-proprietary wireless communications protocol may be used.

Figure 2 shows the device in use. There are two wand devices 10, 11, each with a proximity conductor 12,13. These conductors are momentarily brought together to allow communication between the devices.

For example, two people may meet for various discussions. During the course of these discussions, it becomes apparent that both parties may benefit from a discussion at the secret level on a particular project. Each party then undertakes a process described in the following steps.

They each authenticate to their respective wands, by entering a pass code identification sequence. In a further embodiment (not shown) the wand includes a biometric authentication device such as a fingerprint scanner which is used for this step, either alone or in combination with the pass code.

Via manipulation of the push buttons or wheel each selects a question to ask the other wand which in this case is do they have "secret" clearance.

Each party touches wands for a period of time until the wand signals via a visual means such as the light bands or an audio tone that sufficient data has been transferred between the wands.

The wands then process the data and then each signals to the respective user either success or failure of verification that the other party has a "secret" clearance. This signalling can be either the trusted band lights, or on the trusted visual display, or a combination. Note that an audio tone is insufficient as this could be spoofed by a number of means.

A user must authenticate to the wand before use. After authentication the user has a certain amount of time to undertake the transaction before the device "times out" and re-authentication is required. The wand is adapted to receive, via the wireless communication link, a secure (e.g. encrypted with authentication functions) "heartbeat" signal from other trusted devices to delay activation of the timeout. This allows for multiple transactions to be conveniently carried out.

In a further embodiment, a badge device as shown in Fig 4 is included. This device is capable of establishing a secure wireless connection to one and only one wand device. Via a secure protocol, it can authenticate and transmit and receive data from a specific wand. Trusted appliances which are able to communicate securely together in a manner such that no other device can intrude are known as an ensemble. There can be only one appliance of each type in an ensemble. In the case of visual checking, the wand transmits information to the active badge appliance in its ensemble. The visual contains a visual identity of the other party. Note that it is essential that the visual transmitted to its ensemble partner is that of the other party, otherwise it may be possible to introduce a spoofing attack. In a further embodiment (not shown) there is a pressure sensitive surface or membrane included in the inductive connector so that actual physical contact with each wand is detected as part of the process. Although the threat is small, this

prevents high energy RF devices from simulating very close proximity to another wand device.

An additional embodiment is illustrated in Fig 5. The credential communication device system can be used for the rapid checking of large numbers of personnel credentials for closed meeting attendance. This is currently typically done by attendees presenting a badge or identification pass. When several hundred are involved, it can overload the guards checking each attendee's credentials. A typical example in Defence is checking participant's clearance level to "secret" for attendance at classified functions. The checking method is accomplished using the steps set out below.

The Guard selects the criteria required for admittance, e.g. secret clearance and communicates this selection to a wand device.

The Guard then inserts the wand 20 into a slot 22 in a passive waveguide device 21. This waveguide restricts the range of the wireless communication link of the guard's wand to the area of the channel 22 of the waveguide.

Each participant, having authenticated to their own wand, swipes or sweeps their wand 26 through the waveguide device as shown in Fig 5. The two wands communicate via their secure wireless communication links. The localisation of the signals by the waveguide provides the guarantee that there is no third party involved in the transaction.

The Guard's device undertakes an interrogation via the wireless communication link as the participant's wand is swept through the waveguide utilising variations of previously described methods and signals either success or failure via a trusted visual means on the Guard's wand accompanied by an optional untrusted audio tone.

An alternative embodiment (not shown) has two receptacles, one for the Guard's wand, and the other for the meeting attendee. The attendee inserts their wand into the designated receptacle and removes it at a given signal. The design of the receptacles is such that the close proximity method is achieved and thus a wireless connection is not needed.

With many wireless implementations, the length of time to gain a "data lock", i.e. the length of time for two devices to recognise each other and set up a transfer link may be of the order of seconds. This is typically too long for the applications in mind. A method of avoiding this delay is for the Guard's wand to transmit to a radius out of the waveguide its synchronisation sequences but only receive data within the waveguide. Another alternative is for the Guard's device to have multiple wireless interfaces to achieve the same effect. This permits other wands in the vicinity to "lock in" before they are swept through the waveguide. When swept through the waveguide they are already synchronised for data transfer.

Throughout this specification the purpose of the description has been to illustrate the invention and not to limit this.

A summary of the features might be said to be

1: A tamper resistant trusted apparatus for the purpose of credential exchange, or credential checking, or credential supply through a point to point connection with like apparatuses comprising at least one trusted switch, and one trusted light indicator, and one proximity conductor which permits momentary contact and data transfer between two apparatuses and optionally an untrusted audio generator.

1.2: A trusted apparatus as in 1 where the proximity conductor is implemented in the form of an induction connection such as a very low power RF transceiver such that very close proximity between like apparatuses is required as to simulate the action of physical touch.

1.2.1: A trusted apparatus as in 1.2 where the induction connector is coated with a thin layer or shell of material to protect the induction connector from damage and weather.

1.3: A trusted apparatus as in 1 where there are three trusted coloured light indicators, a wireless connection, a wheel press button, and a trusted display.

1.3a: A trusted apparatus as in 1 or 1.3 which has a biometric authentication device installed.

1.3.1: A trusted apparatus as in 1.3 where the trusted coloured light indicators are formed as bands around the apparatus so that the lights can be viewed easily from multiple angles.

2: A tamper resistant trusted apparatus for the purpose of credential exchange, or credential checking, or credential supply through a point to point connection with like apparatuses, comprising at least one trusted switch, and one trusted light indicator, and one contact connector which permits momentary contact between two apparatuses, and at least one wireless means comprising RF or infrared means and optionally an untrusted audio generator.

2.1: A trusted apparatus as in 2 where the contact conductor is implemented in the form of an induction connection such as a very low power RF transceiver such that very close proximity between like apparatuses is required as to simulate the action of physical touch.

2.1.1: A trusted apparatus as in 2.1 where the induction connector is coated with a thin layer or shell of material to protect the induction connector from damage and the weather.

2.3: A trusted apparatus as in 2 where there are three trusted coloured lights indicators, a wheel press button, and a trusted display.

2.3a: A trusted apparatus as in 2 or 2.3 which has a biometric authentication device installed.

2.3.1: A trusted apparatus as in 2.3 where the trusted coloured light indicators are formed as bands around the apparatus so that the lights can be viewed easily from multiple angles.

2.3.1: A process of mutual suspicion user selected credential exchange utilising a pair of apparatuses as in 2.3 or 1.3 and the process comprising the following steps:

a: each user selects a question to be asked of the other user through the manipulation of the wheel button and viewing the question to be asked from the trusted display;

b: each user then touches the other apparatus for a length of time until the apparatus signals either through the light, trusted display, or an audio tone, or a combination thereof that sufficient data exchange has taken place;
c: Each apparatus signalling success or failure either through one or more or light indicators, or trusted display, or a combination thereof coupled with an optional untrusted audio tone.

2.3.1.1: A process of mutual suspicion credential exchange as in 2.3.1 with an additional process in between b and c where the wand applies an organisational mandatory security policy to the user selected question.

2.3.1.2: A process of mutual suspicion credential exchange as in 2.3.1 with an additional process in between b and c where the wand applies a stored user discretionary security policy.

2.3.1.3: A process of mutual suspicion credential exchange as in 2.3.1 with two additional processes in between b and c where the wand applies a user discretionary security policy and then applies a mandatory security policy.

3: A trusted apparatus as in 2 where rapid group clearance checking is possible by the following process:
a: Checker selects admittance criteria;
b: Checker inserts apparatus in a device which acts as a localiser for the wireless connection such as a passive waveguide;
c: Users pass or sweep their apparatus through the waveguide;
d: Inserted apparatus interrogates via its wireless connection the sweeping apparatus and compares against admittance criteria;
e: Inserted apparatus signals checker of success or failure via one or more of the trusted visual indicators. The visual indicator can optionally be accompanied via an untrusted audio tone.

2.4: A trusted apparatus as in 2 which acts as a component in a mutually authenticated ensemble of devices and where it may signal a trusted badge visual display device to display data.

2.5: A trusted apparatus as in 2 which can activate via a trusted encrypted means the button apparatus in the ensemble to enable the transmission or receiving of audio to and from the button apparatus to other components in the ensemble.

2.3.2: Trusted apparatuses as in 2.3 where mutual suspicion visual identity credentials are checked by the following process:
a: each user authenticates themselves to their trusted apparatus;
b: each user selects the identity credential transfer level to be permitted through the manipulation of the wheel button or trusted switches or a combination thereof;
c: each user then undertakes momentary contact between the trusted apparatuses until such time the apparatuses signal via visual means, or audio means, or a combination thereof that sufficient data transfer has taken place;
d: each trusted apparatus signals via secure wireless means to the trusted badge apparatus in its own ensemble a visual depiction of the other user along with any other necessary data.

2.3.3: Trusted apparatuses as in 2.3 where each apparatus is notified of current mandatory security policies in force by the following process:
a: User manipulates wheel button or trusted buttons or a combination thereof to signal trusted apparatus that current security context is sought;
b: Trusted apparatus signals for a trusted device to supply it with current context;
c: Trusted device may respond with current context.

2.3.4: Trusted apparatuses as in 2.3 where one or more apparatuses are notified of current mandatory security policies in force by the following process:
a: Trusted apparatus on coming into range of a trusted device holding mandatory security policy authority is becomes aware of its presence via its wireless means;
b: Encrypted and authenticated exchange takes place to obtain current mandatory security policy via its wireless means.

4: A trusted apparatus as in 1 or 2 in which the contact conductor is formed as a bulbous tip to permit momentary contact from a variety of angles.

4.1 A trusted apparatus as in 4 where the basic form of the apparatus forms the shape of a cylinder.

4.1.1 A trusted apparatus as in 4.1 where one or more trusted lights form one or more light bands surrounding the circumference of the cylinder.

4.2 A trusted apparatus as in 4 where the contact conductor also forms part of the shaft of the cylinder adjacent to the tip

5: A trusted apparatus as in 1 or 2 where the contact conductor forms part of the shaft of the cylinder to permit momentary contact from a variety of angles.

5.1: A trusted apparatus as in 5 where the basic form of the apparatus forms the shape of a cylinder.

6: A trusted apparatus as in 2 where the apparatus has a timeout which causes the requirement for a re-authentication sequence.

6.2: A trusted apparatus as in 6 where the timeout can be delayed via a secure "heartbeat" signal from another device in the ensemble.

7: A trusted apparatus as in 1 where the apparatus has a timeout which causes the requirement for a re-authentication sequence.

Dated this 11th day of June 2003

THE COMMONWEALTH OF AUSTRALIA

By his Patent Attorneys

COLLISON & CO

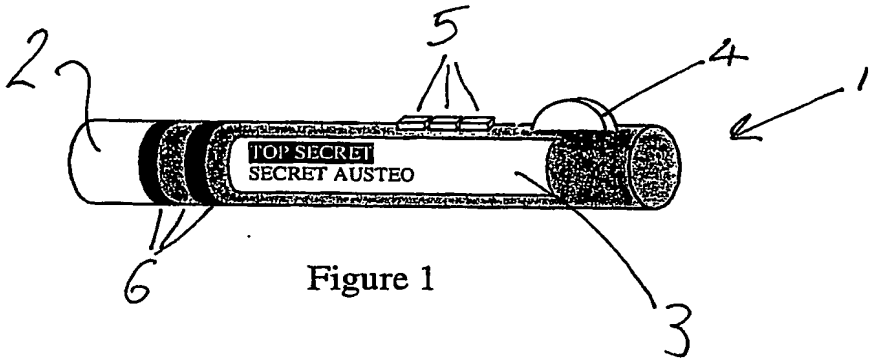

Figure 1

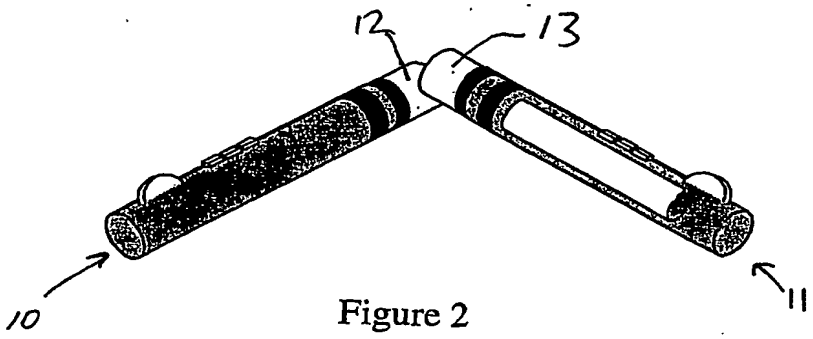

Figure 2

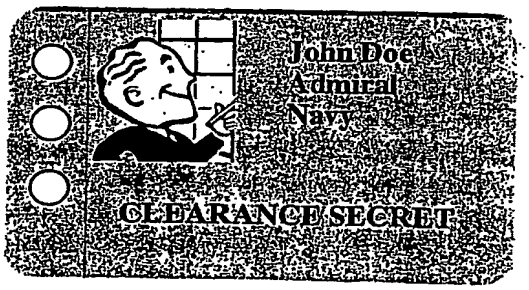

Figure 3

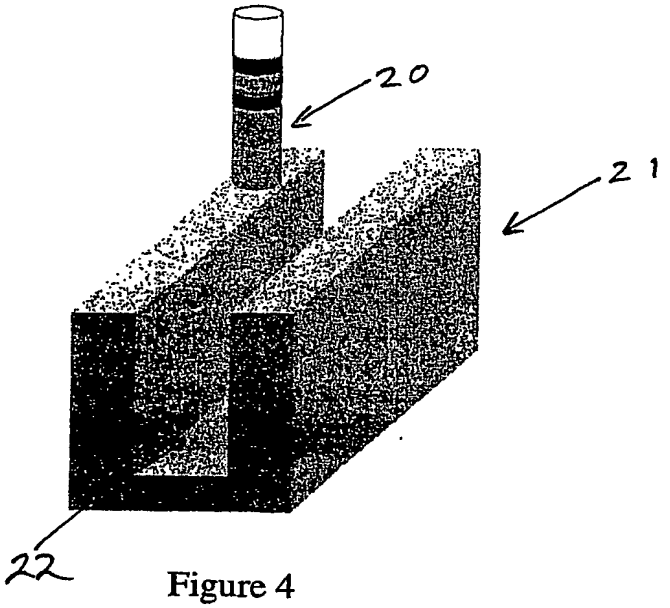

Figure 4

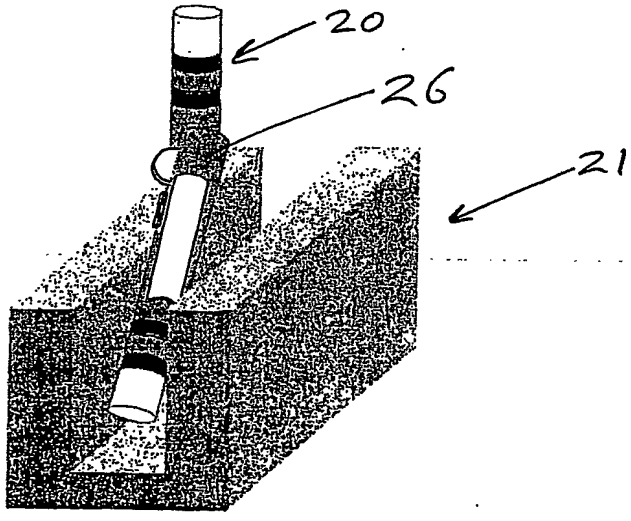

Figure 5